UNIVERSITI TEKNOLOGI MARA

SYN FLOOD DETECTION VIA MACHINE LEARNING

MUHAMMAD MUHAIMIN AIMAN BIN MAZLAN

BACHELOR OF COMPUTER SCIENCE (Hons)
DATA COMMUNICATION AND NETWORKING

JANUARY 2018

Universiti Teknologi MARA

Syn Flood Detection Via Machine Learning

Muhammad Muhaimin Aiman Bin Mazlan

Final Year Project Report submitted in fulfilment of the requirements for
Bachelor of Computer Science (Hons) Data Communication and Networking
Faculty of Computer and Mathematical Sciences

January 2018

SUPERVISOR'S APPROVAL

SYN FLOOD DETECTION VIA MACHINE LEARNING

By

MUHAMMAD MUHAIMIN AIMAN BIN MAZLAN
2015165025

This final year project proposal was prepared under the supervision of the project supervisor, Mohamad Hafiz bin Khairuddin. It was submitted to the Faculty of Computer and Mathematical Science and was accepted in partial fulfillment of the requirements for the degree of Bachelor in Computer Sciences (Hons) Data Communication and Networking.

Approved by

…….
Mohamad Hafiz Bin Khairuddin
Project Supervisor

JANUARY 3, 2018

STUDENT DECLARATION

I certify that this report and the project to which it refers to is the product of my own work and that any idea or quotation from the work of other people, published or otherwise are fully acknowledged in accordance with the standard referring practices of the discipline.

…….
Muhammad Muhaimin Aiman Bin Mazlan
2015165025

JANUARY 3, 2018

ABSTRACT

In the era of technology, Firewall have become an important component for protecting interconnection of the computer resource and network environment. Recently, one the most popular attack is denial of service (DoS) that attempt to be malicious pattern to compromise a server or a network resource. The current problem and issue regarding of existing project is cannot handle the attack by shutdown the connection between inbound and outbound network. Therefore, the aim of this project is to develop a firewall software called "FIREARMS" that can prevent one type of DDoS which is SYN-Flood attack. The core detection and prevention algorithm which is the support vector machine (SVM) were implemented in this project. The software will be trained by using NSL KDD Cup dataset in order to make it learns about the Neptune attack and as a result, it will be able to detect and prevent such attack. The significant of this project is it can be detect any of the SYN-Flood attack accurately and avoid many of false alarm rate. In a conclusion, the software would be able to prevent the computer from SYN-Flood attack by using FIREARMS software. This will help user to secure their network during the connection of their computer to the internet.